NETSTAT :

affiche les statistiques du protocole et les connexions TCP/IP courantes

Syntaxe : netstat [-a] [-ens] [-p protocol] [-r] [interval]

-a	affiche toutes les connexions, les connexions serveurs ne sont en général pas montrées
-e	affiche les statistiques Ethernet, peut être combiné avec l'option –s
-n	affiche les adresses et les n° de port en numérique
-s	affiche les statistiques par protocole, par défaut pour TCP, UDP, ICMP, IP utiliser –p pour spécifier un sous-ensemble de ces protocoles
-p protocol	affiche les connexion pour le protocole spécifié, tcp ou udp avec l'option –s, affiche les statistiques (tcp, udp, icmp,ou ip)
-r	affiche le contenu de la table de routage
interval	réaffiche les statistiques à intervalle régulier taper Ctrl-C pour stopper

Résultats de la commande :

Foreign Address	adresse IP et n° de port du host distant auquel le socket est connecté, le nom est affiché au lieu de l'adresse IP s'il est trouvé dans le fichier HOSTS, si le port n'est pas connecté, son n° est remplacé par *
Local Address	adresse local et n° de port utilisé, le nom est affiché au lieu de l'adresse IP s'il est trouvé dans le fichier HOSTS, si le port n'est pas connecté, son n° est remplacé par *
Proto.	le nom du protocole utilisé par la connexion
(state)	indique le status de la connexion TCP :

- close_wait
- closed
- established
- fin_wait_1
- fin_wait_2
- listen
- syn_received
- syn_send
- timed_wait
- last_ack

exemple :

Connexions actives

Proto	Adresse locale	Adresse distante	état
TCP	truc:1078	216.239.213.138:80	ESTABLISHED
TCP	truc:1079	216.239.213.138:80	ESTABLISHED
TCP	truc:1080	216.239.213.138:80	ESTABLISHED
TCP	truc:1081	216.239.213.138:80	ESTABLISHED
TCP	truc:nbsession	linux7:1033	ESTABLISHED

NBTSTAT :

affiche les statistiques du protocole et les connexions TCP/IP utilisant NetBIOS sur TCP/IP

Syntaxe : nbtstat [-a RemoteName] [-A IP_address] [-c] [-n] [-R] [-r] [-S] [-s] [interval]

-a	Liste la table de noms d'un host distant en donnant son nom
-A	Liste la table de noms d'un host distant en donnant son adresse IP
-c	Liste la table de noms NetBIOS du cache local, avec les adresse IP correspondantes
-n	Liste les noms NetBIOS locaux. “Registered” indique que le nom a été enregistré sur ce nœud du réseau, par broadcast ou par serveur WINS
-R	Recharge le fichier LMHOSTS après purge de tous les noms NetBIOS du cache
-r	Liste les statistiques de résolution de noms pour les réseaux Windows. Sur un PC configuré pour utiliser WINS, cette option retourne le nombre de noms résolus et enregistrés par broadcast ou par WINS
-S	Affiche les sessions station et serveur, liste les hosts distants par adresse IP
-s	Affiche les sessions station et serveur, essaie de convertir les adresses IP des hosts distants en noms par le fichier HOSTS
interval	Ré-affiche les statistiques choisies, pause après chaque affichage. Taper Ctrl-C pour arrêter l'affichage. Si cette option n'est pas choisie, les statistiques ne sont affichées qu'une fois.

Entête des colonnes générées par Nbtstat :

Input	Nombre d'octets reçus
Output	Nombre d'octets émis
In/Out	connexion entrante ou sortante
Life	le temps restant avant qu'un nom entré dans le cache ne soit purgé
Local Name	The local NetBIOS name associated with the connection.
Remote Host	le noim ou l'adresse IP associé au host distant
Type	type de nom : nom unique ou nom de groupe
<03>	chaque nom NetBIOS a 16 caractères de long. Le dernier octet a une signification spéciale, parce que le même nom peut être présent plusieurs fois sur un PC. Cette colonne indique le dernier octet du nom en hexa (20 = espace en ascii).

Status des connexion NetBIOS :

Accepting	une session entrante est en train d'être acceptée et va être connectée
Associated	un point de connexion a été créé et associé avec une adresse IP
Connected	la session a été établie
Connecting	la session est dans la phase de connexion, dans laquelle le mapping nom-adresse IP du destinataire a été résolu
Disconnected	le host local a entamé une déconnexion et attend confirmation du host distant
Disconnecting	une session est en phase de déconnexion
Idle	ce point de connexion a été ouvert, mais ne peut pas recevoir de connexions
Inbound	une session entrante est en phase de connexion
Listening	ce point de connexion est disponible pour une connexion entrante
Outbound	une session est en phase de connexion, la connexion TCP a été créée
Reconnecting	une session est en cours de reconnexion, après un premier essai infructueux

PING :

vérifie les connexions vers un ou plusieurs hosts distants

Syntaxe : ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

-t	Ping vers l'host distant jusqu'à interruption
-a	ne résoud pas les adresses en noms
-n count	envoie un nombre spécifié de paquets echo (4 par défaut)
-l length	envoie des paquets echo contenant un nombre spécifié d'octets de données (64 par défaut, maxi 8192).
-f	envoie le flag "Do Not Fragment" dans le paquet
-i ttl	place le "TTL" à la valeur spécifiée
-v tos	place le "Type Of Service" à la valeur spécifiée
-r count	enregistre la route du paquet sortant et du paquet retour dans le champ "Record Route". Il faut spécifier un minimum de 1 et un maximum de 9 hosts
-s count	spécifie le "time stamp" pour le nombre de hops spécifié par "count"
-j host-list	route les paquets selon la liste de hosts spécifiée, des hosts consécutifs peuvent être séparés par des routeurs intermédiaires, le maximum d'adesses IP est de 9
-k host-list	route les paquets selon la liste de hosts spécifiée, des hosts consécutifs peuvent être séparés par des routeurs intermédiaires (route stricte), le maximum d'adesses IP est de 9
-w timeout	spécifie un intervalle de time-out en ms
destination-list	spécifie les hosts distants à pinguer

Note sur Ping

La commande PING vérifie les connexions vers host(s) distant(s) en envoyant des paquets ICMP echo vers ces hosts et en attendant "echo reply".
Ping attend la réponse pendant 1s et affiche le nombre de paquets envoyés et reçus.
Par défaut, 4 paquets de 64 octets sont émis (séquence de données alphabétique)

On eut utiliser PING ave des noms ou des adresses IP.
Si la comande ne fonctionnepas sur le nom, il peut y avoir un problème de résolution de noms. Dans ce cas, vérifier la base de données du fichier HOSTS ou du DNS.

exemple :

```
C:\>ping ds.internic.net

Pinging ds.internic.net [192.20.239.132] with 32 bytes of data:

Reply from 192.20.239.132: bytes=32 time=101ms TTL=243
Reply from 192.20.239.132: bytes=32 time=100ms TTL=243
Reply from 192.20.239.132: bytes=32 time=120ms TTL=243
Reply from 192.20.239.132: bytes=32 time=120ms TTL=243
```

TRACERT :

Ce test détermine la route vers une destination en envoyant des paquets ICMP echo en variant le TTL vers le destinataire.
Chaque routeur décrémente le TTL Quand le TTL arrive à 0, un message d'erreur (time exceeded) est renvoyé par le routeur.
Notez que certains routeurs détruisent les paquets sans envoyer de message d'erreur et sont donc invisibles dans tracert.

Syntaxe : tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

-d	spécifie de ne pas résoudre les adresses en noms (gain de temps)
-h maximum_hops	spécifie un nombre maxi de hops pour chercher la cible
-j host-list	spécifie une route de sorce perdue selon host-list.
-w timeout	attend un nombre de ms maxi pour chaque réponse
target_name	spécifie le nom de host pour la destination

Notes sur Tracert

L'exemple suivant montre le résultat de tracert.
La 1re colonne est le nombre de hops (TTL dans le paquet émis).
Les 3 colonnes suivantes montrent le délai aller-retour en ms pour chaque test (un * indique temps dépassé).
La 4e colonne indique le nom du destinataire, s'il a étérésolu et l'(adresse IP qui a répondu.

C:\>tracert ds.internic.net

```
Tracing route to ds.internic.net [198.49.45.10]
over a maximum of 30 hops:

1  <10 ms <10 ms   *    [131.107.1.100]
2   10 ms <10 ms  10 ms seattle1-gw.nwnet.net [192.80.12.82]
3    *     10 ms  10 ms enss143-enet.nwnet.net [192.35.180.2]
4   20 ms   *     10 ms t3-3.seattle-cnss8.t3.ans.net [140.222.88.4]
5   30 ms  30 ms  20 ms t3-0.los-angeles-cnss8.t3.ans.net [140.222.8.1
6   70 ms  70 ms  80 ms t3-0.new-york-cnss24.t3.ans.net [140.222.24.1]
7   80 ms  81 ms  80 ms t3-0.denver-cnss40.t3.ans.net [140.222.40.1]
8  100 ms  91 ms  90 ms t3-1.new-york-cnss32.t3.ans.net [140.222.32.2]
9   90 ms  90 ms  91 ms mf-0.new-york-cnss36.t3.ans.net [140.222.32.196]
10 100 ms  90 ms  91 ms t1-0.enss222.t3.ans.net [140.222.222.1]
11 140 ms  191 ms 100 ms ds.internic.net [198.49.45.10]

Trace complete.
```